REMARKS

Claims 1-35 are pending in the present application. By this Response, claims 1, 5, 6, 9, 10-15, 17, 21, 22, 25, 26, 27-31, and 33-35 are amended. Claims 4 and 20 are canceled. Claims 1, 17 and 33 are amended to include the features of claims 4 and 20 and to recite "wherein the access control list controls access to the first managed resource and at least one second managed resource of the plurality of managed resources at a level below the first managed resource in the hierarchy, without directly associating a copy of the access control list with the at least one second managed resource." This feature is supported at least on page 14, lines 15-25 of the current specification. Claims 5 and 21 are amended to be consistent with claims 1 and 17.

Claims 6, 22 and 34 are amended to recite "wherein the first managed resource is a first level resource and the first access control list controls access, by a first entity, to the first managed resource and the at least one second level resource based on the first set of permissions, and wherein the first access control list controls access to the first managed resource and the at least one second level resource, without directly associating a copy of the first access control list with the at least one second level resource." This feature is supported at least on page 14, lines 15-25 of the current specification. Claims 9 and 25 are amended to be consistent with claims 6 and 22.

Claims 10 and 26 are amended to recite "wherein the second access control list controls access to the second managed resource and the at least one subresource without directly associating a copy of the second access control list with the at least one subresource." Claims 11, 27 and 35 are amended to incorporate features of claims 12 and 28 and to recite "wherein the access control list includes a set of permissions for performing a set of operations on the first managed resource and at least one second managed resource of the plurality of managed resource at a level above the first managed resource in the hierarchy, and wherein the access control list is not directly associated with the first managed resource." These features are supported at least on page 14, lines 15-25 of the current specification. Claims 12, 13, 15, 28, 29, and 31 are amended to be consistent with claims 11 and 27.

Claims 14 and 30 are amended to recite "selecting the access control list, from the first access control lists and the second access control list, with a permission that least specifically matches the user." This feature is supported at least on page 13, lines 19-24 of the current specification. No new matter is added as a result of the above amendments. Reconsideration of the claims in view of the above amendments and the following remarks is respectfully requested.

I. 35 U.S.C. § 112, Claims 7-9 and 23-25

The Office Action rejects claims 7-9 and 23-25 under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as invention.

With regard to claims 7-8, and 23-24, the Office Action states that here is insufficient antecedent basis for the "first entity" in the claims. By this Response, claims 6 and 22 are amended to include the phase "by a first entity" to provide sufficient antecedent basis for claims 7-8 and 23-24.

Regarding claims 9 and 25, the Office Action alleges that there is insufficient antecedent basis for "privileges" in the claim. By this Response, claims 9 and 25 are amended to recite "wherein the first set of permissions comprises a set of operations that may be performed for the at least one first level resource." Therefore, sufficient antecedent basis is provided for claims 9 and 25.

II. 35 U.S.C. § 102(b), Claims 1-14, 16-30, and 32-35

The Office Action rejects claims 1-14, 16-30 and 32-35 under 35 U.S.C. § 102(b) as being allegedly anticipated by Glasser et al., (U.S. Patent No. 5,956,715). This rejection is respectfully traversed.

As to claims 1, 17 and 33, the Office Action states:

> Regarding claims 1, 17, and 33, Glasser discloses a method, an apparatus and a computer program product for administering managed resource; and attaching an access control list to an object that represents the managed resource, wherein the access control list assigns at least one

privilege from the set of privileges to an entity. See Col.1, lines 54-58, col. 4, lines 36-65, and col. 7, lines 5-12.
Office Action dated March 24, 2004, page 2.

Independent claim 1, which is representative of independent claims 17 and 33 with regard to similarly recited subject matter, reads as follows:

> 1. A method for administering managed resources, comprising:
> defining a set of privileges for a first managed resource, wherein the first managed resource is one of a plurality of managed resources arranged in a hierarchy; and
> attaching an access control list to an object that represents the first managed resource, wherein the access control list assigns at least one privilege from the set of privileges to an entity; and
> wherein the access control list controls access to the first managed resource and at least one second managed resource of the plurality of managed resources at a level below the first managed resource in the hierarchy, without directly associating a copy of the access control list with the at least one second managed resource.
> (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re bond*, 910 F .2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 21 U.S.P.Q.2d 1031, 1034 (Fed Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F .2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Glasser does not teach every element of the claimed invention arranged as they are in claims 1, 6, 17 and 33. Specifically, Glasser does not teach an access control list that controls access to the first managed resource and at least one second managed resource of the plurality of managed resource at a level below the first managed resource in the hierarchy, without directly associating a copy of the access control list with the at least one second managed resource.

Glasser teaches an approach to manage file and other resource security in a network computing environment. The resource is organized as a hierarchy of

elements with a root element at the top of the hierarchy and additional elements below the root element. A request is received to change a protection, such as an access permission, of an element of the resource hierarchy (other than root) with respect to a particular network user. If the element in question lacks an associated access control list, a nearest ancestor element of the hierarchy is located that has an associated access control list. The first (descendant) element inherits the access control list of the second (ancestor) element. This inheritance is done by generating a copy of the access control list of the second element and associating the generated copy with the first element. The requested change in protection is then incorporated into the generated copy that has been associated with the first element so as to establish an updated access control list of the first element. Further, the requested change can be propagated downwards in the hierarchy from the first element to its descendents having access control lists (Abstract).

However, Glasser does not teach or suggest an access control list that controls access to the first managed resource and at least one second managed resource of the plurality of managed resource at a level below the first managed resource in the hierarchy, without directly associating a copy of the access control list with the at least one second managed resource. As described in the Abstract above, Glasser teaches a descendent element that inherits an access control list from the ancestor element if no access control list is associated with the descendent element. The inheritance is done by generating a copy of the access control list of the ancestor and associating the generated copy with the descendent. Thus, in Glasser, the access control list controls access to the descendent and the ancestor by directly associating a copy of the access control list with the descendent. Glasser does not teach an access control list that controls access to the ancestor element (first managed resource) and the descendent element (at least one second managed resource of the plurality of managed resource at a level below the first managed resource in the hierarchy) without directly associating a copy of the access control list with the descendent element (at least one second managed resource).

In the presently claimed invention, an access control list may be attached to an object representing managed resource. The access control list may control not only access to the first managed resource, but also access to a second managed resource at a level below the first managed resource in the hierarchy. For example, on page 14, lines 17-25 of the current specification, ACL 562 may be created and attached to resource A. This ACL would control management of groups B1, B2, C1 and C2, which are resources in the hierarchy at a level below resource A. Thus, multiple groups of resources maybe managed by a single access control list. This removes the need to associate access control lists with every group in the system.

To the contrary, using Glasser's approach, an access control list is still required for each resource in the hierarchy, since descendent elements in Glasser inherit the access control list from an ancestor by copying the access control list of the ancestor and associating the generated copy with the descendent. Glasser still does not solve the problems with the need to associate access control lists with every resource in the system. Therefore, Glasser does not teach an access control list that controls access to the first managed resource and at least one second managed resource of the plurality of managed resource at a level below the first managed resource in the hierarchy, without directly associating a copy of the access control list to the at least one second managed resource, as recited in claim 1.

Glasser also does not teach a first access control list that controls access to the first managed resource and the at least one second level resource, without directly associating a copy of the first access control list with the at least one second level resource, as recited in claim 6. The Office Action alleges that Glasser teaches that the first access control list controls access to the first managed resource and the at least one second level resource based on the first set of permissions at column 7, lines 5-27, which reads as follows:

> Each folder hierarchy **400** can have an associated permissions list called an access control list (ACL). An ACL for a given folder contains a list of users (and user groups) and their respective access permission for that folder. The folder's ACL is checked each time that any remote user

attempts to access the folder or its contents. ACLs are stored in registry **167** and are managed by file security component **166**. A folder's access permissions can be inherited by its descendants in hierarchy **400**. For example, if folder **420** has an ACL that denies all access permissions to a given user, and folders **421** and **422** lack ACLs of their own, then folders **421** and **422** inherit the permissions of the parent folder **420** and so cannot be accessed by that user. As another example, if folder **401** has an ACL that provides read access for a given user, folder **410** lacks an ACL, folder **411** lacks an ACL, and folder **412** has its own ACL, then folders **410** and **411** inherit the permissions of their ancestor folder **401** with respect to that user, but folder **412** uses its own ACL. Thus, the ACL of folder **412** overrides the ACL that would otherwise be inherited from folder **401** in this example. (The root folder **401** has no ancestors and therefore does not inherit in this embodiment).

In the above section, Glasser teaches how permissions or ACLs are inherited by descendent folders **410** and **411** when folders **410** and **411** lack access control lists. At column 8, line 66 to column 9, line 3, Glasser teaches that in the case where the folder inherits from an ancestor, a copy of the ancestor's is made and the modified copy becomes the folder's new ACL. Thus, Glasser teaches copying an access control list of an ancestor and directly associating the copy with the descendent when the descendent lacks ACL of its own. Glasser does not teach a first access control list that controls access to the first managed resource and the at least one second level resource, without directly associating a copy of the first access control list with the at least one second level resource, as recited in claim 6.

In view of the above, Applicants respectfully submit that Glasser does not teach or suggest all of the features of claims 1 and 6. Independent claims 17, 22, 33 and 34 recite similar features to that of claims 1 and 6 and thus, distinguish over Glasser for similar reasons. At least by virtue of their dependency on claims 1, 6, 17 and 22 respectively, Glasser does not teach or suggest the features of claims 2, 3, 5, 7-10, 18, 19, 21, 23-26. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 1-3, 5, 6-10, 17-19, 21-26 and 33-34 under 35 U.S.C. § 102(b).

In addition, Glasser does not teach or suggest the specific features of dependent claims 2, 3, 5, 7-10, 18, 19, 21, 23-26. For example, Glasser does not

teach or suggest the specific features of amended dependent claims 10 and 26, which now recite "wherein the second access control list controls access to the second managed resource and the at least one subresource without directly associating a copy of the second access control list with the at least one subresource."

As discussed previously in arguments for claims 1 and 6, Glasser teaches copying the ACL of an ancestor if the descendent does not have ACL of its own. Thus, Glasser copies the ancestor's ACL and associates the generated copy of the ancestor's ACL to the descendent, in order to control access of a particular user to the descendent. This is contrary to features of the access control list as recited in claims 10 and 26, which controls access to the second managed resource and the at least one subresource without directly associating a copy of the second access control list with the at least one subresource. Therefore, Glasser does not teach the features of claims 10 and 26. In view of the above, Applicants respectfully submit that Glasser does not teach or suggest each and every feature recited in dependent claims 2, 3, 5, 7-10, 18, 19, 21, 23-26. Thus, Applicants respectfully request withdrawal of the rejection of claims 2, 3, 5, 7-10, 18, 19, 21, 23-26 under 35 U.S.C. § 102(b).

As to independent claim 11, which is representative of claims 27 and 35 with regard to similarly recited subject matter, Glasser does not teach an access control list that includes a set of permissions for performing a set of operations on the first managed resource and at least one second managed resource of the plurality of managed resources at a level above the first managed resource in the hierarchy, and wherein the access control list is not directly associated with the first managed resource.

The Office Action alleges that Glasser teaches these features at column 10, lines 15-29, which reads as follows:

> Once the appropriate ACL has been determined, peer server **120** uses file security component **166** in conjunction with component **168** to compute the user's permissions for the selected folder in the ACL (step DJ). If the user is not listed by name in the ACL, but the ACL contains one or more groups names, a list of user groups previously stored by component **168** can be used to determine the user's group membership; if the user is not among the locally stored groups, a further check can be made with security provider **190** to see whether the user has

rccently been added to any groups. If the user has permission for the requested access (step DK), access is granted (step DL); otherwise, access is denied (step DM). Peer server **120** can perform step DK using either or both of components **165** and **168**, and performs step DL and DM using component **165**.

In the above section, Glasser merely teaches how access of a selected folder is granted for a user in the ACL. While access to the selected folder is granted based on the ACL, Glasser does not teach that the access control list includes a set of permissions for performing a set of operations on the first managed resource and at least one second managed resource of the plurality of the managed resources at a level above the first managed resource in the hierarchy, or that the access control list is not directly associated with the first managed resource.

To the contrary, at column 7, lines 7-8, Glasser teaches that an ACL for a given folder contains a list of users (and user groups) and their respective access permissions for that folder. Glasser's ACL only includes permissions for the folder that is associated with the ACL. Glasser's ACL does not include permissions for other folders. In addition, Glassner's ACL is directly associated with a particular folder. Even with the assumption that Glasser's ACL is inherited by a descendent from an ancestor, the ACL may include permissions for both the ancestor and the descendent. However, the Glasser's ACL is still directly associated with the descendent, since the descendent's ACL is a generated copy of the ancestor's ACL and associated with the descendent. Therefore, Glasser does not teach an access control list that includes a set of permissions for performing a set of operations on the first managed resource and at least one second managed resource of the plurality of managed resources at a level above the first managed resource in the hierarchy, and wherein the access control list is not directly associated with the first managed resource, as recited in claims 11, 27 and 35.

In view of the above, Applicants respectfully submit that Glasser does not teach or suggest each and every feature recited in independent claims 11, 27 and 35. At least by virtue of their dependency on claims 11 and 27 respectively,

Glasser does not teach or suggest the features of claims 12-14 and 28-30. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 11-14 and 27-30 under 35 U.S.C. § 102(b).

In addition, Glasser does not teach or suggest the specific features of dependent claims 12-14 and 28-30. For example, Glasser does not teach or suggest the specific features of amended dependent claims 14 and 30, which recites "wherein the step of determining whether the operation is permitted for the user comprise selecting the access control list, from the first access control list and the second access control list, with a permission that least specifically matches the user."

The Office Action alleges that Glasser teaches these features at column 10, lines 15-29, which is reproduced above. In the above section, Glasser only teaches determining user's permissions for the selected folder in the ACL by first determining whether the user is listed by name in the ACL. If the user is not in the ACL, a list of user groups previously stored in the ACL can be used to determine the user's group membership. If the user is not in the list of groups, other groups may be used to determine whether the user has recently been added to any group. Thus, the step of determination is expanding from a name in the ACL to a list of user groups in the ACL and then to any other groups. Glasser therefore teaches selecting a permission that is more specifically matches the user. Glasser does not teach selecting a permission that is least specifically matches the user.

In the presently claimed invention, for example, on page 13, lines 12-24 of the current specification, a user may be given more or fewer permission than the group to which he or she belongs. Alternatively, the authorization server may stop the search in the ACL with the least specific match, depending on the administration policy. For example, the user "boss" may be limited to helpdesk permissions when "boss" may be limited to helpdesk permissions when "boss" is logged in as a member of the "helpdesk" group. Thus, a user logged in as a member of "helpdesk" may be given fewer permission than when the user is logged in as a user "boss". Glasser does not teach such features. Glasser only

teaches selecting a permission that is most specifically matches the user, not the least specifically matches the user, as recited in claims 14 and 30.

In view of the above, Applicants respectfully submit that Glasser does not teach or suggest each and every feature recited in dependent claims 12-14 and 28-30. Thus, Applicants respectfully request withdrawal of the rejection of claims 11-14 and 27-30 under 35 U.S.C. § 102(b).

III. 35 U.S.C. § 103(a), Alleged Obviousness, Claims 15 and 31

The Final Office Action rejects claims 8 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Glasser et al. (U.S. Patent No. 5,956,715) in view of Abadi (U.S. Patent No. 5,315,657). This rejection is respectfully traversed.

Abadi is directed to an access control list for determining the access rights of principals in a distributed system to a system resource wherein the access rights of a specified principal are based on the access rights delegated to that principal (Abstract). As described in previous arguments, Glasser does not teach or suggest each and every feature of independent claims 11 and 27, from which claims 15 and 31 depend. In addition, Abadi also does not teach the features recited in independent claims 11 and 27. Abadi only teaches granting access to objects using an ACL. Abadi teaches that when a principal requests access to an object, that object's reference monitor attempts to locate the requesting principal's identity in the ACL for that object. If the principal's identifiy is found, the access requested by the principal is compared to the access allowed by the ACL entry.

If the ACL entry indicates that the access requested is allowed, then access is granted. If the requested access is not allowed, then access is not granted. If the principal cannot be found in the ACL, then access is denied. However, Abadi does not mention anything about a hierarchy of objects, let alone an access control list that includes a set of permissions for performing a set of operations on the first managed resource and at least one second managed resource of the plurality of managed resources at a level above the first managed resource in the hierarchy. Therefore, Abadi also does not teach the features recited in claims 11 and 27. Since claims 15 and 31 depend on

claims 11 and 27 respectively, neither Glasser nor Abadi, either alone or in combination, teaches or suggests the feature of claims 15 and 31.

In addition, Abadi does not teach the specific features as recited in claims 15 and 31. The Office Action admits Glasser does not teach performing an OR operation on the first set of operations and the second set of operations, however, the Office Action alleges that Abadi teaches these features in Figure 10 and column 18, lines 22-58, which reads as follows:

> **FIG. 10** also illustrates a third form that an access right expression may take. In this expression, the principal set **82** is listed with no access rights. The listing of a principal-set with no access rights implies that the specified principals are granted all possible access rights.
>
> The principal-sets discussed above may comprise a listing of principal names, a group, or a construct of principals and/or groups. For purposes of this specification, the term "principal-set" will refer to a list of principal names, while the term "NAME" will refer to a group.
>
> When a listing of principal-set comprises a listing of principals, each of the listed principals is granted the access rights indicated by the access right expression. For example, in **FIG. 11**, principals BOB, JOHN, and CARL are all given the access right S, as are all of the principals in group ONE.
>
> Four principal-set constructs are utilized in the embodiment illustrated here. Each will be discussed separately.
>
> a. Principal-set OR Principal-set: The UNION of Groups. The constructs A OR B, where A and B are principal-sets, means that A and B are both members of the set. In other words, to be allowed access, the accessor must be either A or B. The following equation illustrates this construct.
>
> A OR B = > S
>
> Principal-set = > access-right
>
> The above caption indicates that both A and B have access right S for the object controlled by the ACL having this access equation. If the principal seeking access is either A or B access right S will be granted. This is because the basic principal-set comprises the union of A and B.

In the above section, Abadi teaches using an OR expression in an ACL to specify access rights of a list of principals. In the above example, either principal A or principal B, which are members of a principal-set, may have access to S. Thus, the OR operations is performed on the accessors or users within a principal-set or a group. The OR operation is not performed on the first set of operations permitted for the user and the second set of operations permitted for the user, as recited in claims 15 and 31.

The first set of operations and the second set of operations are operations that the user may perform on a managed resource. For example, on page 13, line 25 to page 14, line 4 of the current specification, a user may be logged in as a member of "hr" and "helpdesk". The first set of operations permitted for the group "hr" are "av", "a" meaning add user and "v" meaning view list of users. The second set of operations permitted for the group "helpdesk" are "wv", indicating that those users are permitted to change a password and view a list of users in the group. When the OR operation is performed on the first and second set of operations, the operations permitted for the users become "wav," which includes viewing a list of users, changing password, and adding users. Thus, the OR operations combine different operations permitted for the user from different groups to which the user belongs.

To the contrary, Abadi teaches using the OR operation to combine or UNION different users within a principal-set. Abadi does not combine different operations permitted for the user from different groups. All of the principals that are ORed in Abadi belong to the same principal set or group. Therefore, Abadi does not teach or suggest the features of claims 15 and 31.

Furthermore, the Office Action alleges that it would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate Abadi's access right expressions (such as OR operation) onto the first set and second set of operations of Glasser so that permissions is correctly determined for the specific user. The Office Action alleges that the motivation would have been to enable the system to perform accurate computing of the user's permission when the user belongs to more than one group of resources. Applicants respectfully disagree.

At column 10, lines 15-29, Glasser teaches that a peer server uses file security component **166** and component **168** to compute user's permissions for a selected folder in the ACL. At column 5, lines 51-67, Glasser teaches that component **166** (FILESEC) checks file folder access permissions. Component **168** (MSSP, NWSP) checks user validity by communicating with security provider **190**. In particular, component **168** can obtain from security provider **190** a list of user groups (collections of users all of whom are subject to the same access permissions with respect to a particular resource or resources) and store this list locally on hard disk **121**. Thus, using Glasser's system, the

file security component only checks a list of users or user groups having the same access permissions of a particular resource to determine whether a user or a group of users have access to that resource. There is no teaching or suggestion that the file security component performs any OR operation on the access permissions.

In addition, there is no need for the file security component of Glasser to perform an OR operation on the access permissions, because the access permissions are the same for the list of users or user groups. Therefore, a person of ordinary skill in the art would not have been led to combine the teaching of Glasser with Abadi to perform an OR operation on the first and second set of operations so that permissions is correctly determined for the specific user, since neither Glasser nor Abadi teaches or suggests performing an OR operation on first and second set of operations.

Furthermore, a person of ordinary skill in the art would not have been motivated to combine the teachings of Glasser with Abadi. Glasser is only concerned with determining whether a user or a group of users with the same access permissions have access to a particular resource. Abadi is only concerned with performing an OR operation on the users within the same group. Neither Glasser nor Abadi is concerned with performing an OR operation on a first set of operations permitted for the user and a second set of operations permitted for the same user, such that accurate computing of the user's permission when the user belongs to more than one group of resources can be achieved. Accordingly, Applicants respectfully request withdrawal of rejection of claims 15 and 31 under 35 U.S.C. § 103(a).

IV. Conclusion

It is respectfully urged that the subject application is patentable over Glasser et al. (U.S. Patent No. 5,956,715) and Abadi (U.S. Patent No. 5,315,657), and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: July 26, 2004

Stephen J. Walder, Jr.
Reg. No. 41,534
Yee and Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants

SJW/im